Abstract of the Disclosure

A method and system for the secure transmission of messages between at least two users of a telecommunications network, using a secret, random binary encryption key, which is used once for encryption. The key is generated in a key generator recorded on at least two portable data media, such as CDs, and then output in this form to the users, each of whom receives one data medium containing the recorded key. The key is not stored in any other location. The users insert the recorded key media into reading devices, which are respectively assigned to telecommunications equipment, e.g., telephones, fax machines, or PCs, employed by the users. When a connection is established, logistics devices, which are also assigned to the telecommunications equipment, check whether the keys were entered properly and whether they correspond to each other. The logistics devices also synchronize the entered keys, or at least portions of the keys, when the information to be transmitted is encrypted and decrypted.